SF-058/PCT

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－271105

(43)公開日　平成10年(1998)10月9日

(51)Int.Cl.[6]		識別記号	FI		
H04L	9/08		H04L	9/00	601A
G09C	1/00	660	G09C	1/00	660A
H04H	1/02		H04H	1/02	E
H04L	9/10		H04L	9/00	621A
	9/14				641

審査請求　未請求　請求項の数13　ＯＬ　（全 7 頁）　最終頁に続く

(21)出願番号　特願平9－304676

(22)出願日　平成９年(1997)11月６日

(31)優先権主張番号　９６１３８２２

(32)優先日　1996年11月13日

(33)優先権主張国　フランス（ＦＲ）

(71)出願人　391000771
トムソン　マルチメデイア　ソシエテ　アノニム
THOMSON MULTIMEDIA S. A.
フランス国，92648　ブローニュ　セデックス，ケ・アルフォンス・ル・ガロ　46

(72)発明者　アルナルド　カンピノ
フランス国，35000　レンヌ，プルヴァル・ド・ラ・リベルテ　28

(72)発明者　ジャンーベルナール　フィッシャー
フランス国，35700　レンヌ，リュ・ド・ヴァンセンヌ　９ａ

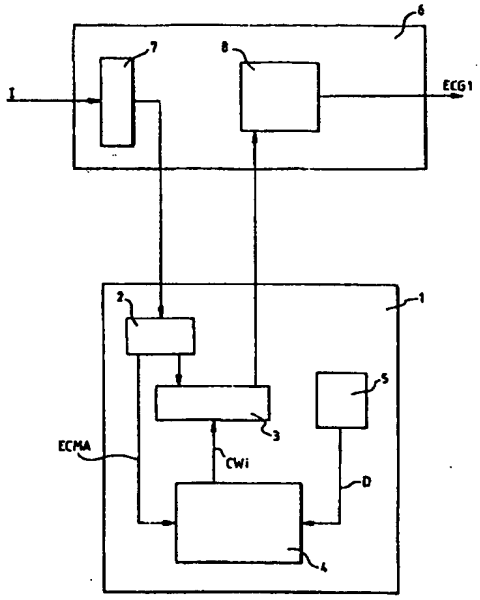
(74)代理人　弁理士　伊東　忠彦　（外１名）

(54)【発明の名称】　セキュリティ要素からデコーダへ伝送される情報アイテムを保護する方法及びそのような方法を使用する保護システム

(57)【要約】

【課題】　ユーザによって選択された番組が暗号化されずに伝送されることによって著作権を侵害されることを防ぐ情報アイテムを保護する方法を提供することを目的とする。

【解決手段】　本発明はセキュリティ要素からデコーダへ伝送された情報アイテムを保護する方法及びそのような方法を使用する保護システムに関する。情報アイテムはデコーダによって情報アイテムが伝送されるべきセキュリティ要素の中で暗号化され、この情報アイテムをデコーダの中で解読することによって保護される。本発明は、条件付きアクセスシステムに適用される。



1

【特許請求の範囲】

【請求項１】　セキュリティ要素（１）に含まれるスクランブル解除装置（３）から生ずるデータのストリームを、セキュリティ要素（１）からデコーダ（６）へ伝送することを可能にし、該データのストリームは条件付きアクセスシステムのユーザによって選択された少なくとも１つの番組を表わしている方法であって、

セキュリティ要素（１）の中で第１の鍵（Ｋ）のアクションの下でスクランブル解除装置（３）から生ずるデータを暗号化することを可能にする第１の段階と、

デコーダ（６）の中で第２の鍵（Ｋ）のアクションの下で該第１の段階から生ずる暗号化された情報アイテムを解読することを可能にする第２の段階とからなることを特徴とする方法。

【請求項２】　第１の段階は、デコーダの中でランダムなワード（ＡＬ）を発生することを可能にする段階と、第１の鍵を発生するような方法で第３の鍵（Ｋ１）のアクションの下でランダムなワード（ＡＬ）を発生することを可能にする段階とからなり、

第２の段階は、ランダムなワード（ＡＬ）を第２の鍵（Ｋ）を発生するように暗号化することを可能にする段階からなることを特徴とする、請求項１記載の方法。

【請求項３】　該第１の段階は、スクランブル解除装置（３）がスクランブル解除するセッションの間に第１の鍵（Ｋ）を構成するようなランダムなワード（ＡＬ）を少なくとも１つ発生することを可能にする段階からなり、

該第２の段階は、暗号化されたランダムなワード（Ｅ（ＡＬ））から形成される情報を形成するよう第４の鍵（Ｋ２）のアクションの下でランダムなワード（ＡＬ）を暗号化する段階と、暗号化されたランダムなワードが第２の鍵（Ｋ）を構成するよう暗号化されたランダムなワード（Ｅ（ＡＬ））を解読する段階とからなることを特徴とする、請求項１記載の方法。

【請求項４】　第１の鍵（Ｋ）は恒久的にユーザカード（１）の中に記憶され、第２の鍵（Ｋ）は恒久的にデコーダ（６）の中に記憶されることを特徴とする請求項１記載の方法。

【請求項５】　制御ワード（CW_i）のアクションの下でスクランブル解除装置（３）によって受信されるデータをスクランブル解除することを可能にするスクランブル解除装置（３）を含み、該データは条件付きアクセスシステムのユーザによって選択された少なくとも１つの番組を表わすセキュリティ要素（１）であって、

第１の暗号化鍵（Ｋ）のアクションの下でスクランブル解除装置（３）から生ずるスクランブル解除された情報アイテムを暗号化する装置（１０）からなることを特徴とするセキュリティ要素（１）。

【請求項６】　ランダムなワード（ＡＬ）のアクションの下で第１の鍵（Ｋ）を発生することを可能にする暗号

2

化鍵を発生する装置（１３）からなることを特徴とする請求項５記載のセキュリティ要素（１）。

【請求項７】　解読鍵（Ｋ２）のアクションの下で第１の鍵（Ｋ）を発生することを可能にする解読装置（１５）からなることを特徴とする請求項５記載のセキュリティ要素（１）。

【請求項８】　セキュリティ要素（１）から生ずるデータを復号化することを可能にし、該データは条件付きアクセスシステムのユーザによって選択された少なくとも１つの番組を表わすデコーダ（６）であって、

第２の鍵（Ｋ）のアクションの下でセキュリティ要素（１）から生ずるデータを解読することを可能にする解読装置（９）からなり、該データは第１の鍵（Ｋ）のアクションの下でスクランブル解除され、暗号化されたデータであることを特徴とするデコーダ（６）。

【請求項９】　少なくとも１つのランダムなワード（ＡＬ）を発生するランダムなワードを発生する装置（１１）と、発生される解読鍵が第２の鍵（Ｋ）であるよう、そのように発生されたランダムなワードから解読鍵を発生する装置（１２）とからなることを特徴とする、請求項８記載のデコーダ（６）。

【請求項１０】　第２の鍵（Ｋ）を形成する少なくとも１つのランダムなワードを発生することを可能にするランダムなワードを発生する装置（１１）と、暗号化鍵（Ｋ２）のアクション下で第２の鍵を形成するランダムなワードを暗号化することを可能にする暗号化装置（１４）とからなることを特徴とする、請求項８記載のデコーダ（６）。

【請求項１１】　セキュリティ要素（１）と、該セキュリティ要素と関連するデコーダ（６）とからなる組立体であって、

セキュリティ要素（１）は請求項６記載のセキュリティ要素であって、デコーダ（６）は請求項９記載のデコーダであることを特徴とする組立体。

【請求項１２】　セキュリティ要素（１）と、該セキュリティ要素と関連するデコーダ（６）とからなる組立体であって、

セキュリティ要素（１）は請求項７記載のセキュリティ要素であって、デコーダ（６）は請求項１０記載のデコーダであることを特徴とする組立体。

【請求項１３】　第１の鍵及び第２の鍵は該組立体に特定的であることを特徴とする請求項１１又は１２記載の組立体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、例えば条件付きアクセスシステムのユーザカードといったセキュリティ要素からデコーダへ伝送される情報アイテムを保護する方法に関する。本発明は更に特定的には、例えば当業者によって「CENELEC/DVB 共通インタフェース」として知ら

れるインタフェース基準に準拠するＰＣＭＣＩＡ型のカード又は米国ＮＲＳＳ（National Renewable Security System）基準に準拠するチップカードといったセキュリティ要素の中でスクランブル解除動作が行われる条件付きアクセスシステムに適用される。

【０００２】

【従来の技術】本発明は、オンライン型又はスタンドアロン型のいずれの条件付きアクセスシステムに対しても適用される。オンライン型の条件付きアクセスシステムでは、スクランブルされた情報アイテムは同時に様々なユーザに分配される信号からなる。

【０００３】スタンドアロン型の条件付きアクセスシステムでは、スクランブルされた情報アイテムは例えばコンパクトディスク又はディジタルビデオディスクといったスタンドアロンの情報媒体上に含まれる。例えばサービスプロバイダといった発信源から生ずる様々な番組を形成する情報アイテムがセキュリティ要素へ伝送される。セキュリティ要素は（セキュリティ素子の中にユーザの権限が存在するという条件の下で）ユーザによって選択された番組をスクランブル解除し、変化されないままにされた他の番組と同じくこの番組をデコーダへ送る。

【０００４】

【発明が解決しようとする課題】上記のような方法は、ユーザによって選択された番組が暗号化されずに伝送されるという欠点を有する。そのような伝送は、海賊版の番組を不法に分配するためにその伝送を使用しうる著作権侵害者によって容易に利用されうる。

【０００５】図１は、従来の技術によるセキュリティ要素／デコーダ組立体を系統的に示す図である。図１のシステムは、情報源Ｉと、デコーダ６と、セキュリティ要素１とからなる。デコーダ６は、復調装置７と、ディマルチプレクス及び復号化装置８とからなる。

【０００６】セキュリティ要素１は、フィルタリング装置２と、スクランブル解除装置３と、アクセス制御装置４と、ユーザ権限記憶装置５とを有する。発信源によって発信された情報アイテムＩは、例えばＭＰＥＧ－２（Moving Picture Expert Group ）トランスポート基準に従う１つ以上の多重化された番組を含む。

【０００７】当業者によって既知であるように、発信源によって出力される番組はスクランブルされた番組である。情報アイテムＩは、以下ＥＣＭと称されるメッセージの中に、解読の後にスクランブルされた番組のスクランブル解除を可能にする暗号化された制御ワードを含む。デコーダが情報アイテムＩを受信した後、情報アイテムＩは装置７によって復調され、次に全体としてセキュリティ要素１へ伝送される。セキュリティ要素は装置２によって、ユーザによって選択された番組に対応するＥＣＭ（図１ではＥＣＭＡと表示）をフィルタリングし、ＥＣＭを処理のために装置４へ伝送する。情報アイテムのフィルタリングされていない部分は修正されることなくスクランブル解除装置３へ伝送される。装置４はＥＣＭを処理するための従来の機能を実行し、特に、選択された番組をスクランブル解除のために必要であり装置５によって出力される権限Ｄが装置４に供給されているという条件の下で、装置４の中の制御ワードＣＷｉを解読する。

【０００８】制御ワードＣＷｉは続いて、ユーザによって選択されたプログラムをスクランブル解除するために制御ワードＣＷｉを使用するディスクランブリング装置３へ伝送される。スクランブル解除装置３によって出力された情報アイテムは、使用可能な、即ち例えば映画の場合に表示可能な情報アイテムＥＣＧ１を発生するよう、ディマルチプレクス及び復号化装置８に伝送される。

【０００９】

【課題を解決するための手段】本発明は上記の欠点を有さない。セキュリティ要素に含まれるスクランブル解除装置から生ずるデータのストリームを、セキュリティ要素からデコーダへ伝送することを可能にする方法に関する。この方法は、セキュリティ要素の中で第１の鍵のアクションの下でスクランブル解除装置から生ずるデータを暗号化することを可能にする第１の段階と、デコーダの中で第２の鍵のアクションの下で該第１の段階から生ずる暗号化された情報アイテムを解読することを可能にする第２の段階とからなる。

【００１０】本発明はまた、制御ワードのアクションの下でスクランブル解除装置によって受信されるデータをスクランブル解除することを可能にするスクランブル解除装置を含むセキュリティ要素に関する。セキュリティ要素は、第１の暗号化鍵のアクションの下でスクランブル解除装置から生ずるスクランブル解除された情報アイテムを暗号化する装置からなる。

【００１１】本発明はまた、セキュリティ要素から生ずるデータを復号化することを可能にし、該データは条件付きアクセスシステムのユーザによって選択された少なくとも１つの番組を表わすデコーダに関する。デコーダは、第２の鍵のアクションの下でセキュリティ要素から生ずるデータを解読することを可能にする解読装置からなり、該データは第１の鍵のアクションの下でスクランブル解除され、暗号化されたデータである。

【００１２】本発明は更に、セキュリティ要素と、デコーダとからなる組立体に関する。セキュリティ要素は上述の本発明によるセキュリティ要素であって、デコーダは上述の本発明によるデコーダである。上述のように、本発明の利点は、セキュリティ要素からデコーダへのユーザによって選択された番組の伝送を保護することからなる。

【００１３】

【発明の実施の形態】本発明の他の特徴及び利点は添付

の図面を参照して本発明の実施例より明らかとなろう。全ての図面において、同じ参照番号は同じ要素を示す。図２は、本発明の第１の実施例によるセキュリティ要素／デコーダ組立体を系統的に示す図である。

【００１４】図１で説明される要素に加え、デコーダ６は解読装置９を有し、セキュリティ要素１は暗号化装置１０を有する。ユーザによって選択された番組は、暗号鍵Ｋを使用して装置１０によって暗号化される。逆に、装置９は同一の鍵Ｋによって番組を解読する。有利なことに、このことはセキュリティ要素とデコーダとの間で暗号化されていない番組が伝送されることを避ける。

【００１５】本発明によれば、暗号化及び解読鍵Ｋは全てのセキュリティ／デコーダの対に共通でありうるが、また夫々のセキュリティ／デコーダの対又はグループに対して特定的であり得る。有利なことに、セキュリティ要素の著作権侵害された複製物の製造は従って減ぜられる。このように、この技術によって、著作権侵害者は各複製物をそれが接続されているデコーダに基づいてカスタマイズさせねばならない。このことは著作権侵害者にとってその仕事を複雑化させ、従って海賊版を作成することによって得られる報酬を減少させる結果をもたらす。

【００１６】図２の実施例の特定的な実施によれば、装置９及び１０に対して公開鍵アルゴリズムが使用されうる。この場合、暗号化鍵は解読鍵とは異なり、望ましい方法では、セキュリティ要素の中での暗号化のために秘密鍵が使用され、一方デコーダの中での解読のために公開鍵が使用されうる。本発明の第１の実施例によれば、鍵Ｋはセキュリティ要素及びデコーダの両方の上に恒久的に記憶された鍵である。

【００１７】図３は、本発明の第２の実施例によるセキュリティ要素／デコーダ組立体を系統的に示す図である。図２に説明された要素に加え、デコーダはランダムな数又はランダムなワードＡＬを発生させるための装置１１と解読鍵を発生するための装置１２とからなり、セキュリティ要素は暗号化鍵１３を発生する装置からなる。

【００１８】図２に示されるように固定の鍵Ｋを使用する代わりに、ここでは暗号化及び解読鍵は動的に発生される。このために、デコーダ６は装置１１によってランダムな数ＡＬを発生し、それをセキュリティ要素の装置１３へ伝送する。更に、装置１１は、ランダムな数を装置１２へ伝送する。装置１２は解読鍵Ｋを与えるよう、鍵Ｋ１のアクションの下、ランダムな数ＡＬを暗号化する。同様に、セキュリティ要素の装置１３は鍵Ｋ１のアクションの下、ランダムな数ＡＬを暗号化し、暗号化鍵Ｋを作り出す。

【００１９】図３に示される本発明の特定的な実施例によれば、装置１２及び１３で使用される暗号化アルゴリズムは鍵Ｋ１と共に「ワンウエイ」機能によって置き換えられうる。そのような機能は、例えば欧州特許出願第９６４０１３３６．１－２２０９号の中に説明されている。有利なことに、装置１２及び１３は、著作権侵害者がデコーダとセキュリティ要素との間を進行するデータアイテムＡＬをのみを通じて暗号化／解読鍵Ｋを発見することを防ぐ。

【００２０】本発明の他の特定的な実施例によれば、装置１３及び１２によって使用される鍵Ｋ１はセキュリティ要素／デコーダの対に対して特定的であり得、従って上述の利点を示す。本発明の他の特定的な有利な実施例によれば、暗号化及び解読鍵Ｋを発生する過程は、セッション毎、又はセッション当たり数回更新されうる。セッションはユーザによる同一の番組の受信の中断されないシーケンスであると理解される。

【００２１】鍵Ｋの更新は、中でも、以下の利点を有する。一方で、更新によって装置９及び１０のアルゴリズムの暗号化／解読の安全性を増加することが可能である。アルゴリズムの安全性は、アルゴリズムが暗号解読法による著作権侵害行為に対する耐性であると理解される。鍵の更新の頻度は、アルゴリズムを暗号解読するために著作権侵害者によって利用可能である同一の鍵によって暗号化されたデータの量に直接影響を与える。この量を制限することは攻撃に対するアルゴリズムの耐性を増加させ、鍵Ｋの頻繁な更新は装置９及び１０の暗号化／解読アルゴリズムの安全性を増加させる。

【００２２】他方では、更新によって以前に選択された番組の再生を避けることが可能である。従って、悪意のあるユーザ又は著作権侵害者が装置１０によって出力された情報を記録し、従って時点ｔにおいてK_tによって示される鍵で暗号化された形式の選択された番組を記録すると、時点ｔ＋Δｔにおける

【００２３】

【外１】

解読鍵$K_{t+\Delta t}$

【００２４】は、暗号鍵K_tとは異なるため、続いて上記の番組を使用することはできない。図４は、本発明の第３の実施例によるセキュリティ要素／デコーダ組立体を系統的に示す図である。図２に示される要素に加え、図４は、デコーダに関してはランダムな数を発生する装置１１及び暗号化装置１４を含み、セキュリティ要素に関しては解読装置１５を含む。

【００２５】発生装置１１は、装置９によって直接解読鍵Ｋとして使用されるランダムな数ＡＬを発生する。更に、ランダムな数ＡＬは、ランダムな数を暗号化し、セキュリティ要素の装置１５へ伝送する装置１４へ伝送される。装置１４によって実行される暗号化は、鍵Ｋ２のアクションの下で実行される。セキュリティ要素側では、暗号化されたランダムな数Ｅ（ＡＬ）が鍵Ｋ２のアクションの下で装置１５によって解読され、その結果のＡＬは暗号化鍵Ｋとして作用するよう装置１０へ伝送さ

れる。

【００２６】本発明の他の実施例によれば、公開鍵アルゴリズムは装置１４及び１５に対して使用されうる。この場合、暗号化鍵は解読鍵とは異なり、望ましい方法では、装置１５の中での解読のために秘密鍵が使用され、同時に装置１４の中での暗号化のために公開鍵が使用される。有利なことに、装置１４及び１５は対称アルゴリズム又は公開鍵アルゴリズムのいずれを使用していても、著作権侵害者が単にＥ（ＡＬ）を知ることによって暗号化／解読鍵Ｋを発見することを防ぐ。

【００２７】上述の本発明の特定的な実施例によれば、ランダムな数ＡＬはセッション毎に１回又は同一セッションの間に数回発生され、装置１４及び１５によって使用される暗号化／解読鍵Ｋ２は、セキュリティ要素／デコーダの対に対して特定的にされ、従って上述の利点を示す。

【００２８】本発明においては、図２、３及び４に示される全ての実施例に対して、装置９及び１０の暗号化／解読アルゴリズムは、番組の保護の所望の水準と、デコーダ及びセキュリティ要素の中で実施されるアルゴリズムの複雑性との折衷の結果、選択される。従って、専用回路を通じて簡単に実施されうる対称アルゴリズムが望ましい。そのような装置は有利に、実施のコストを減少させ、例えば約１０メガビット毎秒のオーダの高い暗号化／解読レートを確実にする。暗号化鍵の更新は有利に、簡単なアルゴリズムの使用と同時に、暗号解読による著作権侵害行為の危険を減少させることを可能にする。

【００２９】更にデコーダの装置９によって実行される系統的な解読は、特定的な利益、即ちユーザがデコーダを通じてセキュリティ要素から発せされる番組のみを表示しうることを示す。これは例えば、暗号化されていない著作権侵害された番組はそれだけではデコーダ上で再生されないことを意味する。鍵Ｋ１及びＫ２が夫々のセキュリティ要素／デコーダの対に対して特定的な場合は、上述の系統的な解読の性質は追加的な利点を有し、即ち著作権侵害者が同一の番組を著作権侵害行為を実施したデコーダと異なるデコーダへ供給することを防ぐ。

【００３０】更に、図２、３及び４に示される全ての実施例に対して、装置８及び９を同一の電子回路の中に集積する実施が望ましい。これは選択された番組の内容が２つの装置の間で暗号化されずに現れることを妨ぎうるためである。

【図面の簡単な説明】

【図１】従来の技術によるセキュリティ要素／デコーダ組立体を系統的に示す図である。

【図２】本発明の第１の実施例によるセキュリティ要素／デコーダ組立体を系統的に示す図である。

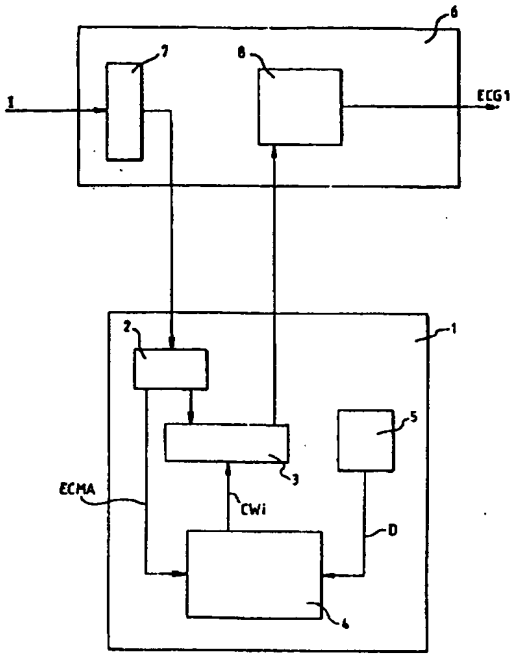
【図３】本発明の第２の実施例によるセキュリティ要素／デコーダ組立体を系統的に示す図である。

【図４】本発明の第３の実施例によるセキュリティ要素／デコーダ組立体を系統的に示す図である。

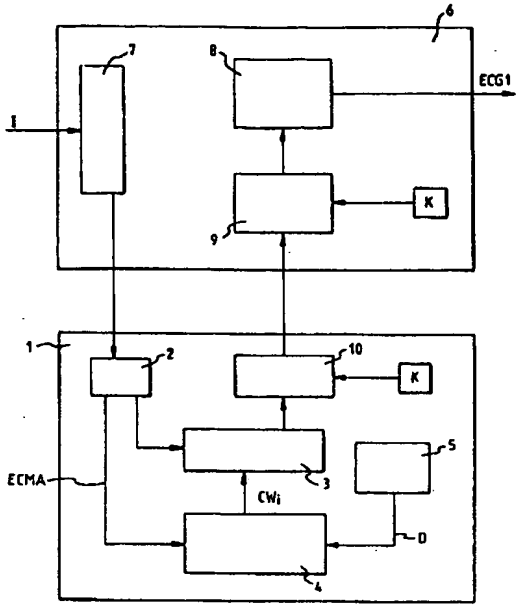
【符号の説明】

１　セキュリティ要素
２　フィルタリング装置
３　スクランブル解除装置
４　アクセス制御装置
５　ユーザ権限記憶装置
６　デコーダ
７　変調装置
８　ディマルチプレクス及び復号化装置
９　解読装置
１０　暗号化装置
１１　ランダムな数／ワード発生装置
１２　解読鍵発生装置
１３　暗号化鍵発生装置
１４　暗号化装置
１５　解読装置

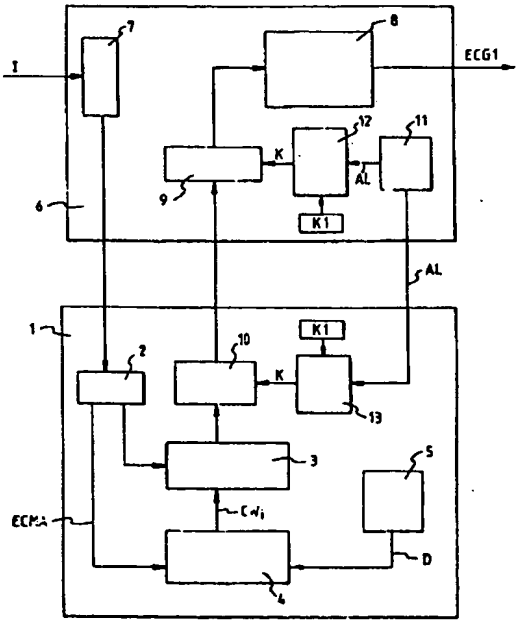
【図１】


6
7
8
I
ECG1
2
1
5
3
ECMA
CWi
D
4

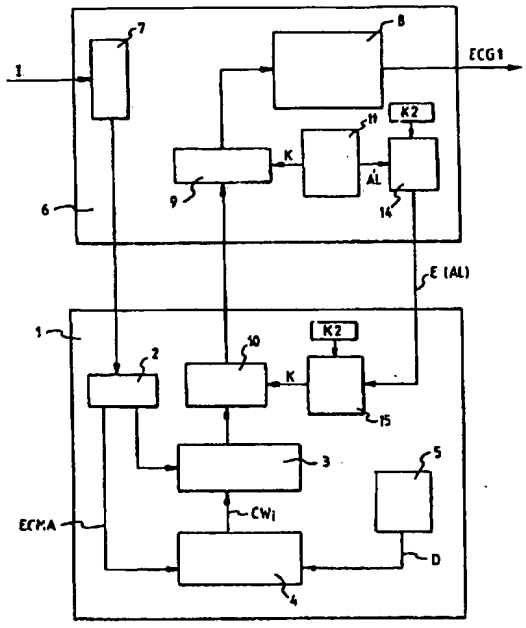
【図２】


6
7
8
ECG1
I
K
9
1
2
10
K
5
ECMA
3
CWi
D
4

【図３】


I
7
8
ECG1
12
11
K
AL
9
K1
6
AL
1
2
10
K1
K
13
3
5
ECMA
CWi
D
4

【図４】


I
7
8
ECG1
K2
19
K
AL
9
14
6
E (AL)
1
K2
2
10
K
15
3
5
ECMA
CWi
D
4

フロントページの続き

(51)Int.Cl.6	識別記号	FI	
H04N 7/167		H04N 7/167	Z